GIS Odyssey Journal

2021 • Volume 1 • Number 2

https://doi.org/10.57599/gisoj.2021.1.2.123

Kamil Czaplicki[1]

SCHENGEN INFORMATION SYSTEM (SIS)

Abstract: The article discusses the principles of functioning of one of the largest databases in the world – the Schengen Information System (SIS). The article describes the history of the creation of the system, its genesis, and the goals it is supposed to achieve. The system's evolution was described, particularly the development of the second-generation system (SIS II). The article presents the basic functionalities of the system and its role in ensuring security and public order. The article presents the definition issues related to information and IT systems.

Keywords: information system, data, identification, border protection

Received: 17 December 2021; accepted: 30 December 2021

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Warsaw, Poland, ORCID ID: 0000-0002-3777-4339, email: k.czaplicki@uksw.edu.pl

The genesis of the SIS

The Schengen Information System (SIS) was created in 1995 as a compensatory measure for abolishing border controls within the European Union. Previous control measures applied at the borders of EU countries monitored the movement of citizens of other countries, eliminated the movement of criminal groups or allowed surveillance of the activity of their citizens. Border controls also ensured the surveillance of goods entering a country (Wagner, 2021). It sought to eliminate the movement of prohibited goods, including those that directly threaten the safety of citizens and the environment. The idea of introducing the free movement of European Union citizens, embodied in the Schengen Agreement signed on 14 June 1985 by five Member States of the European Union, entailed a high risk of breaching the security of European Union Member States through the uncontrolled movement of both persons and goods. The Schengen Information System was intended to compensate for the abolition of border controls using possible data checks on EU citizens and certain goods (O.JL2000.239.13) (Schengen Agreement done by Five Mebers – Belgium, Holland, Luxmbourg, Germany and France). According to Article 92 of the Convention implementing the Schengen Agreement of 14 June 1985, the purpose of the Schengen Information System was to enable the authorities designated by the parties to the Convention, through an automated search procedure, to have access to alerts on persons and property for border checks and other police and customs checks carried out within the country under national law and, in specific cases, to issue visas, residence permits and the administration of legislation on aliens in the context of the application of the provisions of the Convention relating to the movement of persons.

Information system

It is worth noting that the system's designers have chosen to use the word "information" in the system's name (THE SCHENGEN INFORMATION SYSTEM). The literature points out that information systems collect, assemble and process information (Szpor, 2016). The Act on Informatisation of Activities of Entities Executing Public Tasks defines an ICT system as a set of cooperating IT devices and software ensuring processing, storing, sending and receiving data through telecommunication networks with the use of a telecommunication end device appropriate for a given type of network, within the meaning of the Act of 16 July 2004 – Telecommunications Law (Szpor, 2010). It should be recognised that the term information system is a broader term than ICT system because it also emphasises hardware and software (hardware and software). It also highlights the importance of content. Szpor considers the translation of "information system" as an IT system in the implemented acts of EU law to be incorrect (an example of incorrect transposition is the NIS Directive). It is worth noting here that this mistake was not made in the case of the system in question, and the SIS is translated correctly as the Schengen Information System. The legislator has deliberately emphasised, not only in its purpose but also in its name, the importance of the content of

the SIS in ensuring the security of the countries of the European Union which are party to the Schengen Implementing Convention.

Design of the SIS

The SIS operating schedule was defined in Article 92 of the implementing Convention. According to this provision, the system was common to all Contracting States. The system consisted of a central unit and national modules, which were the same in all the Member States. Data from each Member State were available to other States to carry out automated searches (Frießem, 1995).

The SIS allowed for verifying two types of items – persons and objects. The catalogue of things that may be entered in the SIS is defined in Article 100 of the Implementing Convention. It includes objects such as vehicles, trailers and semi-trailers which have been stolen, misappropriated or lost, firearms which have been stolen, misappropriated or lost, blank official documents which have been stolen, misappropriated or lost, issued identity papers that have been stolen, misappropriated or lost and suspect banknotes.

In the case of persons for whom an alert has been issued, the issuing State should include, among other things, the surname and given names and possible aliases, any specific physical characteristics not subject to change, date and place of birth, sex, nationality, information on potential weapons and aggressiveness of the person. Furthermore, the reason for the alert and the proposed course of action should be given if the person is found. There are many reasons for putting data of a person to the SIS. It could be a person wanted for extradition detention, a missing person; a person sought to be summoned to appear before the judicial authorities, aliens who have been refused entry on the grounds of reasonable threat to public policy, public security or national security. In addition, the system records persons who should be subject to secret surveillance or special checks. Under Article 99 of the CISA, such an alert may be issued for persons in respect of whom there is clear evidence that the person intends to commit a criminal offence or where an overall assessment of the person concerned made, inter alia, based on past criminal offences, gives reason to suppose that that person will commit a particularly serious criminal offence in the future.

The second generation Schengen Information System (SIS II)

The benefits of the Schengen Information System, including the opportunity to make the vision of free movement within the countries integrated into the system more tangible, meant that more and more countries wanted to join the SIS. Initially, the Schengen area consisted of five countries (France, Germany, Belgium, the Netherlands and Luxembourg). On 26 March 1995, Spain and Portugal also joined the system. Although not a member of the European Union, Monaco has its borders with France removed. Later on, Italy (26 October 1997) and Austria (1 December 1997) joined the Schengen Information System. On 16 October 1997, Vatican City and San Marino, which, although not a member of the EU, have abolished their borders with Italy, became

members of the Schengen Agreement. Greece joined the SIS on 26 March 2000, followed by Finland, Denmark, Sweden on 25 March 2001. Finland, Denmark, Sweden. Subsequently Norway and Iceland, which are not members of the European Union, also joined the SIS. The great interest in the system meant that its outdated infrastructure was no longer sufficient. There were an increasing number of interruptions in the system's operation, which made it extremely difficult to carry out checks and controls in the system properly. The European Union authorities created a new system, the so-called SIS II Generation (Tomaszewski & Girdwoyń, 2018). The new system was to be five times more efficient than the previous system, would allow 30 countries to be connected and would have twice the data coverage of the first-generation SIS (Dragan, 2015).

Legal basis of SIS II

The legal basis for the operation of the second generation Schengen Information System is Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ EU L.381.4) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ EU L.205.63 of 2007.08.06). In addition, detailed rules on the operation of SIS II are described in Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ EU 312, of 7.12.2018, pp. 1–13), Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending the Convention Implementing the Schengen Agreement and amending and repealing Regulation (EC) No 1987/2006 (Dz. EU OJ L 312, 7.12.2018, pp. 14–55) and Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (EU OJ L 312, 7.12.2018, pp. 56–106).

The purpose of SIS II was to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories, using information communicated via this system.

Poland joined the Schengen Information System on 21 December 2007. Poland was joined by Hungary, Slovenia, Slovakia, Latvia, Malta, Lithuania and Estonia, and a year later by Switzerland, which is not a member of the European Union. The last country to

join the Schengen Information System was Liechtenstein, which joined on 19 December 2001 (Huybreghts, 2015).

The legal basis for Poland's participation in the system was the Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System. The legal basis for Poland's participation in the system was the Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System.

Data processed in the SIS II

Similar to the first generation of SIS, the technical architecture of SIS II comprised a central system (consisting of a database, a support function, the SIS II database and a uniform national interface), a national system (N.SIS.II) and an encrypted communication infrastructure between the central and the national systems (Bufon, 2015). The central system is located in Strasbourg, France, with a central backup system in Sankt Johann im Pongau, Austria, to take over a central unit failure fully (Dragan, 2015). The national systems are built, operated and maintained with national resources. Each Member State was obliged to designate an authority responsible for running its national system (N.SIS II). The role of the designated authority was the smooth operation and security of the national component. In addition, each country was to establish a so-called SIRENE Bureau to ensure the exchange of all information into the system. A very important aspect of developing the second generation of SIS was the interoperability of the national components. According to Article 9 of Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation, and use of the second generation Schengen Information System (SIS II), each Member State establishing its N. SIS II was to comply with protocols and technical procedures established at the central level. Compliance with these protocols was to ensure the compatibility of N. SIS II with the central system.

Member States were also obliged to ensure data security (Czaplicki, 2018), including among others ensuring physical protection of data by drawing up contingency plans for the protection of critical infrastructure, prevent unauthorised access to data-processing facilities used for processing personal data (infrastructure access control), prevent unauthorised reading, copying, modification or removal of data media (data media control, prevent unauthorised input of data and unauthorised inspection, modification or deletion of stored personal data (storage control) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control), ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control); ensure that all authorities with a right of access to SIS II or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the national supervisory authorities without delay,

ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control), ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when by whom and for what purpose the data were input (input control), prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media, in particular by means of appropriate encryption techniques (transport control), monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).

In the second generation system, the scope of data processing has been significantly extended. With regard to persons, these are surnames and forenames, name at birth, previously used forenames and surnames, any specific objective physical characteristics not subject to change, place and date of birth, sex, photographs, fingerprints, nationality, whether the person is armed, violent or a fugitive, reason for the alert, the authority issuing the alert, reference to the decision giving rise to the attention, type of offence, action to be taken following disclosure of the person concerned.

According to the Act on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System, access to the data collected in the SIS II is available to courts, the prosecutor's office, the Head of the Office for Foreigners, the Police, the Customs and Fiscal Service, the Internal Security Agency, the Military Police, the Central Anti-Corruption Bureau, the Border Guard, the Foreign Intelligence Agency, the Military Counterintelligence Service and the Military Intelligence Service, the director of the maritime office. The Polish authority responsible for the national system N. SIS II is the central technical body of the National IT System KSI. The supervision over the operation of the national component is exercised by the Minister competent for internal affairs. Additionally, the President of the Office for Personal Data Protection shall be entitled to direct access to the National IT System to control the compliance of the processing of personal data in the system with the binding provisions.

The SIS II will collect data on, e.i., persons wanted for arrest for surrender purposes based on a European Arrest Warrant (Velicogna, 2014); persons wanted for arrest for extradition purposes; missing persons to be placed under protection or whose whereabouts need to be ascertained (Sołtyszewski & Solodov, 2021); persons whose presence is required for proceedings, including witnesses, persons summoned or sought to be summoned to appear before the judicial authorities in connection with criminal proceedings to account for acts for which they are being prosecuted; persons who are to be served with a criminal judgment or other documents in connection with criminal proceedings to account for acts for which they are being prosecuted; persons who are to be served with a summons to report to serve a penalty involving deprivation of liberty. The SIS II also contains data on aliens who have been refused entry into the territory of a Member State.

Summary

The SIS II database is of great importance for the security of the Schengen area. Every citizen of the European Union has the right to move freely without going through a long and complicated border control procedure. However, this freedom has not caused States to lose full control over the security of their territories. Anyone who enters the Schengen area can be checked, and their details are contained in the SIS II system. The exchange of information between individual states reflects the integration of the Schengen area and contributes to even greater cooperation between the associated countries.

References

Act of 24 August 2007 on the participation of the Republic of Poland in the Schengen Information System and the Visa Information System (Dz.U. 2021 item 1041).

Act on Informatisation of Activities of Entities Executing Public Tasks of 17 February 2005 (Dz.U. 2021 item 2070).

Bufon M. (2011). Engineering Borders and Border Landscapes: The Schengen Regime and the EU's New Internal and External Boundaries in Central-Eastern Europe. In: S. Brunn (ed.). Engineering Earth. Springer, Dordrecht, pp. 2067–2087, https://doi.org/10.1007/978-90-481-9920-4_114 [access: 09.12.2021].

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ EU L.205.63 of 2007.08.06).

Czaplicki K. (2018). Security of Geographical Information system – How to ensure their Confidentiality, Integrity, Availability and Resilience? In: Geographic Information System Conference and Exhibition "GIS ODYSSEY", Italy, pp. 142–145.

Dragan A. (2015). System Informacyjny Schengen drugiej generacji jako nowoczesne rozwiązanie informatyczne (*The second generation Schengen Information System as a modern IT solution*). Annales Universitatis Mariae Curie-Skłodowska, Lublin, Sectio G. Ius, vol. 62, no. 1, pp. 35.

Frießem P. (1995). Global Management for a Real European Information System taking the Schengen Information System (SIS) as an example. In: F. Huber-Wäschle, H. Schauer, P. Widmayer (ed.), GISI 95. Informatik aktuell. Springer, Berlin, Heidelberg, pp. 110–117, https://doi.org/10.1007/978-3-642-79958-7_14 [access: 09.12.2021].

Huybreghts G. (2015). The Schengen Convention and the Schengen *acquis*: 25 years of evolution. ERA Forum 16, pp. 379–426, https://doi.org/10.1007/s12027-015-0402-3 [access: 09.12.2021].

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ EU L.381.4).

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ EU 312, of 7.12.2018, pp. 1-13).

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending the Convention Implementing the Schengen Agreement and amending and repealing Regulation (EC) No 1987/2006 (Dz. EU OJ L 312, 7.12.2018, pp. 14–55).

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (EU OJ L 312, 7.12.2018, pp. 56–106).

Sołtyszewski I., Solodov D. (2021), Międzynarodowa współpraca Policji w obszarze poszukiwań osób zaginionych (*International Police cooperation in the field of searching for missing persons*). In: E. Gruza, I. Sołtyszewski (ed.), Poszukiwania osób zaginionych (*Search for missing persons*), Warszawa, pp. 260–262.

Szpor G. (2010). The Electronic Platform of the Public Administration Services. In: D. Kereković (ed.), Space, Heritage & Future. Croatian Information Technology Association – GIS Forum, Uniwersity of Silesia, Zagreb, pp. 274–281.

Szpor G. (2016). Jawność i jej ograniczenia. Tom I. Idee i pojęcia (*Disclosure and its limitations. Volume I. Ideas and concepts*), C.H. Beck, Warszawa, pp. 120–125.

Tomaszewski T., Girdwoyń P., Europejska Przestrzeń Kryminalistyczna (*European Forensic Space*). In: Ł. Pisarczyk (ed.), Prawne problemy i wyzwania Unii Europejskiej (*Legal problems and challenges of the European Union*), Warszawa, pp. 257–274.

Velicogna M. (2014). The Making of Pan-European Infrastructure: From the Schengen Information System to the European Arrest Warrant. In: F. Contini, G. Lanzara (ed.), The Circulation of Agency in E-Justice. Law, Governance and Technology Series, vol. 13. Springer, Dordrecht, pp. 185–215, https://doi.org/10.1007/978-94-007-7525-1_8 [access: 09.12.2021].

Wagner J. (2021). Border Management in Europe. In: Border Management in Transformation. Advanced Sciences and Technologies for Security Applications. Springer, Cham, pp. 169–192, https://doi.org/10.1007/978-3-030-62728-7_7 [access: 09.12.2021].